

05-09-02

Gp 12152,
#2

PATENT

ATTORNEY DOCKET NUMBER: 1007-022

Express Mail Label No. EV025380066US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Chia Chi Feng	Group Art Unit:	2152
Serial No.:	10/090,181	Examiner:	Unknown
Filed:	3/2/2002	Attorney Docket No.:	1007-022
Title: SYSTEM AND METHOD FOR ELECTRONIC FILE TRANSMISSION			

**TRANSMITTAL OF PRIORITY DOCUMENT FOR FILED APPLICATION UNDER
35 USC 119(b)**

Commissioner for Patents
Washington, D.C. 20231

RECEIVED**MAY 13 2002**

Sir/Madam:

Technology Center 2100

The Petitioner hereby submits a Certified Copy of the Priority Document for the above-referenced application. The priority application number 090117505 was filed in Taiwan, Republic of China, on July 18, 2001.

Transmitted herewith are the documents for the above-identified application:

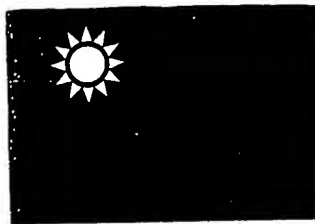
- ☒ Priority Document Taiwan Application 090117505
- ☒ Acknowledgement Postcard
- ☒ No additional fee is required

At any time during the pendency of this application, please charge any fees required or credit any overpayment to Deposit Account 50-0374 pursuant to 37 CFR 1.25.

Respectfully submitted,

Mikio Ishimaru
Reg. No. 27,449
May 6, 2002

The Law Offices of Mikio Ishimaru
1110 Sunnyvale-Saratoga Road, Suite A1
Sunnyvale, CA 94087-2554



中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

RECEIVED

MAY 13 2002

Technology Center 210C

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下：

This is to certify that annexed is a true copy from the records of this
office of the application as originally filed which is identified hereunder:

申請日：西元 2001 年 07 月 18 日
Application Date

申請案號：090117505
Application No.

申請人：文化傳信科技（澳門）有限公司
Applicant(s)

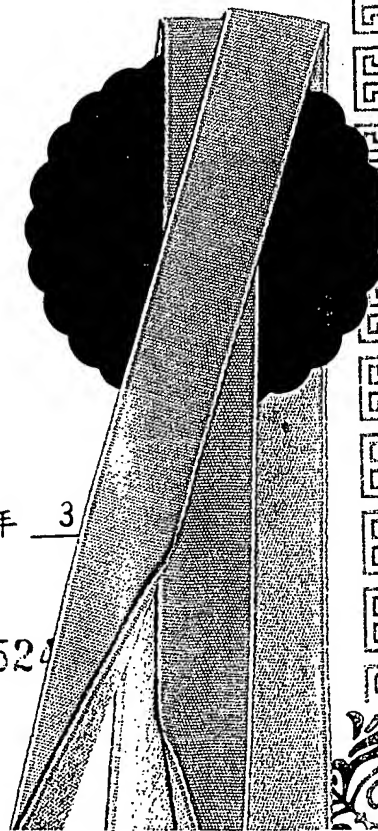
CERTIFIED COPY OF
PRIORITY DOCUMENT

局長
Director General

陳明邦

發文日期：西元 2002 年 3
Issue Date

發文字號：0911100524
Serial No.



申請日期	
案 號	
類 別	

A4
C4

(以上各欄由本局填註)

發明專利說明書

一、發明 名稱	中 文	一種電子檔案傳輸系統及方法
	英 文	
二、發明 創作人	姓 名	封家麒
	國 籍	中華民國
	住、居所	澳門新口岸洗星海大馬路珠光大廈 6 樓 J-L 座
三、申請人	姓 名 (名稱)	文化傳信科技(澳門)有限公司
	國 籍	澳門
	住、居所 (事務所)	澳門路環黑沙海灘龍爪角路 15 號
	代 表 人 姓 名	朱邦復

裝

訂

線

四、中文發明摘要（發明之名稱：一種電子檔案傳輸系統及方法）

一種電子檔案傳輸系統及方法，係應用於網路環境中，當檔案經由網路進行傳輸時，以電子檔案讀取裝置所含之硬體序號予以加密，並以點對點通訊協定來進行傳輸，使電子檔案讀取裝置的使用者能上傳加密檔案以及下載加密檔案，並且由於檔案之加密/解密方式，使得下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，檔案於儲存時，仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，而並非以解密檔案的型式將檔案予以儲存。此電子檔案傳輸系統包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置。電子檔案傳輸系統之傳輸網路為一般的網際網路，負責居中讓檔案處理中心以及電子檔案

英文發明摘要（發明之名稱：）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

四、中文發明摘要（發明之名稱：

讀取裝置之間，能進行上傳、下載加密檔案。進行電子檔案傳輸方法時，於註冊程序，檔案處理中心將得到電子檔案讀取裝置之硬體序號；於檔案上傳過程時，電子檔案讀取裝置將利用其硬體序號為加密鑰匙，而將檔案予以加密，並傳送給檔案處理中心，檔案處理中心接收到此經硬體序號加密之檔案後，將對其所具有之資料庫進行搜尋，以找出傳送端之電子檔案讀取裝置所對應的硬體序號，而對加密檔案予以解密，以得出檔案內容；於進行檔案下載過程時，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，對下載檔案予以加密，並傳送給提出請求之電子檔案讀取裝置。於進行檔案讀取過程時，提出請求之電子檔案讀取裝置於接收到此加密檔案後，將以

英文發明摘要（發明之名稱：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

四、中文發明摘要（發明之名稱：_____）

其自身獨有的硬體序號，對此經加密之檔案予以解密，而得出檔案內容。本發明之電子檔案傳輸系統及方法，於接收端之電子檔案讀取裝置下載經硬體序號予以加密之檔案後，對下載之加密檔案進行讀取時，以其本身之硬體序號做為解密鑰匙，而讀出解密後之檔案內容，且本發明之電子檔案傳輸系統及方法，使得電子檔案讀取裝置所下載之檔案，檔案僅在被讀取時為解密狀態；當儲存於電子檔案讀取裝置，磁片，或光碟片時，下載檔案為加密狀態；所以，即便非接收端之電子檔案讀取裝置得到此些加密檔案後，由於所具有的硬體序號不相同，所以並不能對加密檔案進行解密讀取，使得下載之檔案，僅能在接收端之電子檔案讀取裝置上，才能予以解密並讀取。

英文發明摘要（發明之名稱：_____）

（請先閱讀背面之注意事項再填寫本頁各欄）

裝

訂

線

五、發明說明(1)

發明領域：

本發明係有關於一種檔案傳輸系統及方法，更詳而言之，係有關於一種傳輸電子檔案之過程中予電子檔案加密與解密之電子檔案傳輸系統及方法。

發明背景：

對於目前的網路終端使用者而言，如果能以一種安全、方便的交易機制，取得數位化的文化資訊，例如，數位化電子書，將會是非常地便捷。出版商可架設訊息伺服器，以供使用者經由網際網路，而下載數位化資訊、電子檔案；對於消費者而言，可以利用電子數位設備，例如，個人電腦，個人數位助理器 PDA，亦或電子書讀取機，來讀取所下載的檔案。

習知的數位化資訊、電子書系統，如第 1 圖中所示，係利用訊息伺服器 11 與個人電腦 13 經由網際網路 12 做網路連結。

數位化資訊提供者，例如出版商，會在訊息伺服器 11 設立一個網站 111，以供使用者下載電子檔案 113，在此，電子檔案 113 可為非加密檔案，當使用者進入網站 111，填寫個人相關資料，並加入會員後，先下載電子書讀取軟體 112，待於使用者端完成安裝讀取軟體 112 後，使用者即可開啟電子書讀取軟體 112，直接在訊息伺服器 11 之網站 111 中，下載電子檔案 113 以進行讀取。

個人電腦 13 對訊息伺服器 11 提出連結請求，進入訊息伺服器 11 之網站 111 並做加入會員的動作，待加入會

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(2)

員後，下載電子書讀取軟體 112，以便讀取出版廠商所提供的數位化資訊。於個人電腦 13 的使用者，欲讀取電子檔案 113 時，首先，先對訊息伺服器 11 的網站 111，提出下載電子檔案 113 的請求。待網站 111 確認於個人電腦 13 之使用者為其會員後，經由網際網路 12，而將電子檔案 113 傳送給個人電腦 13。於個人電腦 13 之使用者得到電子檔案 113 後，將用電子書讀取軟體 112，來對電子檔案 113 進行讀取。於個人電腦 13 之使用者可將電子檔案 113 儲存於個人電腦 13 內，亦或將電子檔案 113 儲存於磁片 131 或光碟片 132。在此種讀取過程中，會發生一種情況，例如，個人電腦 14 對訊息伺服器 11 提出連結請求，進入訊息伺服器 11 之網站 111 並做加入會員的動作，待加入會員後，下載得到電子書讀取軟體 112。而當於個人電腦 14 之使用者欲讀取電子檔案 113 時，可無須經由網際網路 12，而向訊息伺服器 11 提出下載電子檔案 113 之請求，而是可經由網際網路 12，以檔案傳輸協定 FTP 方式，自個人電腦 13 而將電子檔案 113 載入個人電腦 14 內；或是直接將載有電子檔案 113 之磁片 131 或光碟片 132，置入個人電腦 14 中，而載入電子檔案 113。待個人電腦 14 載入電子檔案 113 後，可用電子書讀取軟體 112，來對電子檔案 113 進行讀取。於個人電腦 14 的使用者，欲讀取電子檔案 113 時，可無須經由訊息伺服器 11，而是經由個人電腦 13 之處取得電子檔案 113。在此，當訊息伺服器 11 之出版商，欲藉由會員下載電子檔案 113 之動作，

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

五、發明說明(3)

而對會員進行收費時，位於個人電腦 14 之使用者，可自個人電腦 13 處而取得電子檔案 113，而無須必定經由訊息伺服器 11 才可取得。

對於另一種習知的習知的數位化資訊、電子書系統，如第 2 圖所示，係利用訊息伺服器 15 與個人電腦 17 經由網際網路 16 做網路連結。

數位化資訊提供者，例如出版商，會在訊息伺服器 15 設立一個網站 151，以供使用者下載數位化資訊，在此，電子檔案 153 將以 128bit 的加密技術，而加密成為加密檔案 154，當使用者進入網站 151，填寫個人相關資料，並加入會員後，先下載電子書讀取軟體 152，待於使用者端完成安裝讀取軟體 152 後，使用者即可開啟電子書讀取軟體 152，直接在訊息伺服器 15 之網站 151 中，下載加密檔案 154，並對加密檔案 154 進行解密動作，以解密得到電子檔案 153 而進行讀取。

個人電腦 17 對訊息伺服器 15 提出連結請求，進入訊息伺服器 15 之網站 151 並做加入會員的動作，待加入會員後，下載電子書讀取軟體 152，以便讀取出版廠商所提供的數位化資訊。於個人電腦 15 的使用者，欲對加密檔案 154 進行解密動作，以解密得到電子檔案 153 而進行讀取時，首先，先對訊息伺服器 15 的網站 151 提出下載加密檔案 154 的請求。待網站 151 確認於個人電腦 17 之使用者為其會員後，經由網際網路 16，而將加密檔案 154 傳送給個人電腦 17。於個人電腦 17 之使用者得到加密檔

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(4)

案 154 後，將用電子書讀取軟體 152，來對加密檔案 154 進行解密動作，以解密得到電子檔案 153 而進行讀取。於個人電腦 17 之使用者可將解密後之電子檔案 153 儲存於個人電腦 17 內，亦或將電子檔案 153 儲存於磁片 171 或光碟片 172。在此種讀取過程中，會發生一種情況，例如，個人電腦 18 對訊息伺服器 15 提出連結請求，進入訊息伺服器 15 之網站 151 並做加入會員的動作，待加入會員後，下載得到電子書讀取軟體 152。而當於個人電腦 18 之使用者欲讀取電子檔案 153 時，可無須經由網際網路 16，無須向訊息伺服器 15 提出下載加密檔案 154 之請求，再以電子書讀取軟體 152 對加密檔案 154 進行解密，得到電子檔案 153，而是可經由網際網路 16，以檔案傳輸協定 FTP 方式，自個人電腦 17 而將電子檔案 153 載入個人電腦 18 內；或是直接將載有電子檔案 153 之磁片 171 或光碟片 172，置入個人電腦 18 中，而載入電子檔案 153。待個人電腦 18 載入電子檔案 153 後，可用電子書讀取軟體 152，來對電子檔案 153 進行讀取。於個人電腦 18 的使用者，欲讀取電子檔案 153 時，可無須經由訊息伺服器 15，而是經由個人電腦 17 之處取得電子檔案 153。在此，當訊息伺服器 15 之出版商，欲藉由會員下載電子檔案 153 之動作，而對會員進行收費時，位於個人電腦 18 之使用者，可自個人電腦 17 處而取得電子檔案 153，而無須必定經由訊息伺服器 15 才可取得。

在此，即便對於電子檔案 153 而言，所採用的加密方

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(5)

式為 128bit 的加密技術，此種經加密後的加密檔案 154，只有在相對應使用的電子書讀取軟體 152 上，才能加以解密讀取。但是，由於加密檔案 154，經電子書讀取軟體 152 解密讀取後，是以非加密的電子檔案 153 的型式予以儲存，無論是存於個人電腦 17，磁片 171，或光碟片 172，所儲存的檔案均為非加密的電子檔案 153，而並非是加密檔案 154。所以，如果使用者將此非加密的電子檔案 153 傳送給其他人，而由於其他人，例如，個人電腦 18 之使用者，所使用的電子書讀取軟體 152 亦相同，所以仍可對電子檔案 153 進行開啟讀取。此處將產生一個問題，即是，於訊息伺服器 15 之出版商無法抑止電子檔案 153 的再複製傳播。

所以在一般習知的數位化資訊的交易、傳送、接收過程中，一般的數位化文件、書籍、資料，並沒有數位化版權管理的概念，亦即，一般的數位化文件、書籍、資料，在上傳亦或下載傳輸過程中，並未經過加/解密動作；而即便是經過加/解密的動作，由於使用相同的電子書讀取軟體，以及加密檔案經解密讀取後，以非加密檔案型式予以儲存，因而，此些數位化資訊可無限制的做複製拷貝，並做再次傳輸散播，對於訊息伺服器提供者，例如，出版商而言，如何去有效地以一種交易機制，在既能保護消費者，亦能保護數位化資訊提供者的立場，能正確並符合公平交易的原則前提下，來完成線上數位化資訊交易，乃是待解決的問題。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(6)

發明概述：

本發明之主要目的便是在於提供一種電子檔案傳輸系統及方法，係應用於網路環境中，當檔案經由網路進行傳輸時，以電子檔案讀取裝置所含之硬體序號予以加密，並以點對點通訊協定來進行傳輸，於電子檔案讀取裝置的使用者能上傳加密檔案、以及下載加密檔案，並且由於檔案之加密/解密方式，使得下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，於儲存檔案時，仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，而並非以解密檔案的型式將檔案予以儲存，而能達到防止數位化資訊無限制的做複製拷貝、並做再次傳輸散播的目的。

根據以上所述的目的，本發明提供了一種新穎之電子檔案傳輸系統及方法，當檔案經由網路進行傳輸時，以電子檔案讀取裝置所含之硬體序號予以加密，並且由於檔案之加密/解密方式，使得下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，於儲存檔案時，仍用硬體序號將已解密讀取之檔案予以加密並做儲存，而能達到防止數位化資訊無限制的做複製拷貝、並做再次傳輸散播的目的。

此電子檔案傳輸系統包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置。電子檔案傳輸系統之傳輸網路為一般的網際網路或企業網路，負責居中讓檔案處理中心以及電子檔案讀取裝置之間，能進行上傳、下載加密檔案。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(7)

檔案處理中心為進行數位化資訊服務的伺服平台，可進行檔案下載、以及儲存上傳檔案的動作。電子檔案讀取裝置則供使用者進行下載、上傳電子檔案之用，其中之每一個電子檔案讀取裝置均有其獨有的硬體序號，各個電子檔案讀取裝置並利用其獨有的硬體序號，以對電子檔案進行解密之用，而無法以別的電子檔案讀取裝置的硬體序號來對電子檔案做解密的動作。於進行電子檔案傳輸方法時，首先，檔案處理中心會記錄各個電子檔案讀取裝置的硬體序號。

檔案處理中心包含檔案加/解密模組，此檔案加/解密模組與一個或一個以上的電子檔案讀取裝置，經由傳輸網路做網路連結，檔案加/解密模組將其公開鑰匙傳送給一個或一個以上的電子檔案讀取裝置；於進行電子檔案下傳時，此檔案加/解密模組，利用電子檔案讀取裝置的硬體序號當成加密鑰匙，並利用對稱性加密方式，來對電子檔案做加密，將此些經對稱性加密方式所加密的電子檔案，經由傳輸網路，而傳送給電子檔案讀取裝置；在電子檔案讀取裝置上傳檔案至檔案處理中心時，此檔案加/解密模組可利用一個或一個以上的電子檔案讀取裝置的硬體序號，並以對稱性解密方式，來對經加密之檔案做解密的動作。

每一個電子檔案讀取裝置均分別地包含一個讀取/傳接處理模組，電子檔案讀取裝置經由傳輸網路，而得到檔案處理中心的公開鑰匙；當電子檔案讀取裝置對檔案處理

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(8)

中心，進行資料、檔案上傳時，此讀取/傳接處理模組利用其本身之電子檔案讀取裝置的硬體序號、以及對稱性加密方式，來對上傳檔案做加密，電子檔案讀取裝置將此加密後之檔案，經由傳輸網路而傳至檔案處理中心；於進行電子檔案下載時，此讀取/傳送處理模組利用電子檔案讀取裝置之硬體序號，以對稱性解密方式，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上，而當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，可儲存於電子檔案讀取裝置之記憶裝置，磁片，亦或光碟片中。

本發明之電子檔案傳輸方法，係首先，進行註冊啟始程序，當電子檔案讀取裝置與檔案處理中心，經由傳輸網路做網路連結後，檔案處理中心將其公開鑰匙，傳送給與其做網路連結的各個電子檔案讀取裝置；各個電子檔案讀取裝置可利用檔案處理中心所發行之公開鑰匙、以非對稱性單向函數加密方式，將經加密處理後之硬體序號，經由傳輸網路而傳送給檔案處理中心。檔案處理中心將利用其私有鑰匙，對經非對稱性單向函數加密方式所加密的電子檔案讀取裝置的硬體序號訊息，進行解密，而得出各個電子檔案讀取裝置之硬體序號，並將此些硬體序號儲存於資料庫內。

於進行檔案上傳過程時，電子檔案讀取裝置之讀取/傳接處理模組，將利用電子檔案讀取裝置之硬體序號，以

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(9)

對稱性加密方式，來對上傳檔案做加密，電子檔案讀取裝置將此加密後之檔案，經由傳輸網路而傳至檔案處理中心。檔案處理中心接收到此經硬體序號加密之檔案後，將搜尋其所具有之資料庫，以找出傳送端之電子檔案讀取裝置所對應的硬體序號，利用檔案加/解密模組而對加密檔案予以解密，以得出檔案內容。

於進行檔案下傳過程時，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，利用檔案加/解密模組，以電子檔案讀取裝置的硬體序號當成加密鑰匙，並利用對稱性加密方式，來對電子檔案做加密，將此些經對稱性加密方式加密的電子檔案，經由傳輸網路，而傳送給電子檔案讀取裝置。電子檔案讀取裝置之讀取/傳接處理模組，利用電子檔案讀取裝置之硬體序號，以對稱性解密方式，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上，而當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，可儲存於電子檔案讀取裝置之記憶裝置，磁片，亦或光碟片中。

由於本發明之電子檔案傳輸系統及方法，其中之檔案上傳、下載，並非利用如習知電子書讀取軟體的加/解密方式，而是利用各個電子檔案讀取裝置所獨有的硬體序號，來對檔案做加/解密動作。於上傳/下載檔案，以硬體序號當成加/解密鑰匙，進行檔案加/解密動作時，由於硬

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明(10)

體序號均不相同，即便將此下載的檔案傳送給其他電子檔案讀取裝置，由於硬體序號的不同，仍無法解密讀取；而當讀取完成後，於儲存檔案時，電子檔案讀取裝置仍以加密方式，將電子檔案予以存檔。

對於每一個電子檔案讀取裝置而言，由於具有不同的硬體序號，因而，即便其他電子檔案讀取裝置在取得下載檔案的情況下，由於所具有的硬體序號的不同，仍無法對下載檔案進行解密讀取，使得下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，於儲存檔案時，仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，而並非以解密檔案的型式將檔案予以儲存。亦即，加密檔案經解密讀取後，以加密檔案型式予以儲存，因而，此些數位化資訊具有不可再次散播讀取性。

圖示簡述：

為讓本發明之上述和其它目的，特徵，優點能更明顯易懂，將舉較佳實施例，並配合所附圖示，詳細說明本發明之實施例，所附圖式之內容簡述如下：

第 1 圖為習知技術之一電子檔案傳輸系統；

第 2 圖為習知技術之另一電子檔案傳輸系統；

第 3 圖為一系統方塊圖，其中顯示應用本發明之電子檔案傳輸系統之一實施例的基本硬體組態架構；

第 4 圖為一系統方塊圖，其中顯示應用本發明之電子檔案傳輸系統之另一實施例的基本硬體組態架構；

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明（ 11 ）

第 5 圖為一示意圖，用以更詳細地解釋於第 3 圖中之電子檔案傳輸系統，進行電子檔案傳輸方法時之資料流向；

第 6 圖為一運作流程圖，其中顯示應用本發明之電子檔案傳輸系統以進行電子檔案傳輸方法的流程程序；

第 7 圖為一運作流程圖，其中顯示於第 6 圖中之進行註冊啟始步驟之流程程序；

第 8 圖為一運作流程圖，其中顯示於第 6 圖中之進行電子檔案傳輸步驟之流程程序；

第 9 圖為一運作流程圖，其中顯示應用如第 3 圖中之電子檔案傳輸系統之實施例，以進行電子檔案傳輸方法的一流程程序；以及

第 10 圖為一運作流程圖，其中顯示應用如第 4 圖中之電子檔案傳輸系統之實施例，以進行電子檔案傳輸方法的另一流程程序。

實施例詳細說明：

第 3 圖為一系統方塊圖，其中顯示應用本發明之電子檔案傳輸系統之一實施例的基本硬體組態架構。如圖中所示，此電子檔案傳輸系統 2 包含檔案處理中心 3、傳輸網路 4、以及電子檔案讀取裝置 5、6。電子檔案傳輸系統 2 之傳輸網路 3 為一般的網際網路或企業網路，負責居中讓檔案處理中心 3 以及電子檔案讀取裝置 5、6 之間，能進行上傳、下載加密檔案。檔案處理中心 3 為進行數位化資訊服務的伺服平台，可進行檔案下載、以及儲存上傳檔案

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

五、發明說明 (12)

的動作。電子檔案讀取裝置 5、6 可為，例如，個人電腦，個人數位助理 PDA，電子書讀取機，供使用者進行下載、上傳電子檔案之用，其中之每一個電子檔案讀取裝置 5、6 均有其獨有的硬體序號，電子檔案讀取裝置 5(6)並利用其獨有的硬體序號，以對電子檔案進行解密之用，而無法以別的電子檔案讀取裝置 6(5)的硬體序號來對電子檔案做解密的動作。

檔案處理中心 3 包含檔案加/解密模組 31，此檔案加/解密模組 31 與電子檔案讀取裝置 5、6，經由傳輸網路 4 做網路連結，檔案加/解密模組 31 將其公開鑰匙 Key32 傳送給電子檔案讀取裝置 5、6。各個電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61 可利用檔案處理中心 3 所發行之公開鑰匙 Key32、以非對稱性單向函數加密方式 Ea，將經加密處理後之含有硬體序號 S52、S62 的資料，經由傳輸網路 4 而傳送給檔案處理中心 3。檔案處理中心 3 之檔案加/解密模組 31 將利用其私有鑰匙 Key33，對經非對稱性單向函數加密方式 Ea 所加密的電子檔案讀取裝置 5、6 的硬體序號 S52、S62 訊息，進行解密而得出各個電子檔案讀取裝置 5、6 之硬體序號 S52、S62，並將此些硬體序號 S52、S62 儲存於資料庫 34 內。

每一個電子檔案讀取裝置 5、6 均分別地包含一個讀取/傳接處理模組 51、61，電子檔案讀取裝置 5、6 經由傳輸網路 4，而得到檔案處理中心 3 的公開鑰匙 Key32；當電子檔案讀取裝置 5、6 對檔案處理中心 3，進行資料、

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (13)

檔案上傳時，此讀取/傳接處理模組 51、61 利用其本身之電子檔案讀取裝置的硬體序號 S52、S62、以及對稱性加密方式 Es，來對上傳檔案做加密，電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61 將此加密後之檔案，經由傳輸網路 4 而傳至檔案處理中心 3；於進行電子檔案下載時，讀取/傳接處理模組 51、61 利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性解密方式 Ds，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案分別展現於電子檔案讀取裝置 5、6 之螢幕 53、63 上，而當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組 51、61 仍用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，將已解密讀取之檔案予以加密並做儲存，可儲存於電子檔案讀取裝置 5、6 之記憶裝置 54、64，磁片 55、65，亦或光碟片 56、66 中。

第 4 圖為一系統方塊圖，其中顯示應用本發明之電子檔案傳輸系統之另一實施例的基本硬體組態架構。如第 4 圖中所示，此電子檔案傳輸系統 7 包含檔案處理中心 71、傳輸網路 72、以及電子檔案讀取裝置 73、74。電子檔案傳輸系統 7 之傳輸網路 72 為一般的網際網路或企業網路，負責居中讓檔案處理中心 71 以及電子檔案讀取裝置 73、74 之間，能進行上傳、下載加密檔案。檔案處理中心 71 為進行數位化資訊服務的伺服平台，可進行檔案下載、以及儲存上傳檔案的動作。電子檔案讀取裝置 73、74 可為，例如，個人電腦，個人數位助理 PDA，電子書讀取機，

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (14)

供使用者進行下載、上傳電子檔案之用，其中之每一個電子檔案讀取裝置 73、74 均有其獨有的硬體序號，電子檔案讀取裝置 73(74)並利用其獨有的硬體序號 S735(S745)，以對電子檔案進行解密之用，而無法以別的電子檔案讀取裝置 74(73)的硬體序號 S745(S735)來對電子檔案做解密的動作。

檔案處理中心 71 包含處理器 711、記憶體 712、資料儲存媒體 713，資料儲存媒體 713 含有檔案加/解密程式 714、以及資料庫 717，處理器 711 可為微處理器或中央處理器，資料儲存媒體 713 可為硬碟，磁片，光碟片，可抹除程式化唯讀記憶體 EPROM，電子式可抹除程式化唯讀記憶體 EEPROM，或快閃記憶體 Flash ROM，處理器 711 可執行檔案加/解密程式 714，以進行上述之檔案加/解密模組之工作。檔案處理中心 71 與電子檔案讀取裝置 73、74，經由傳輸網路 72 做網路連結，檔案處理中心 71 將其公開鑰匙 Key715 傳送給電子檔案讀取裝置 73、74。各個電子檔案讀取裝置 73、74 之讀取/傳接處理程式 734、744 可利用檔案處理中心 3 所發行之公開鑰匙 Key715、以非對稱性單向函數加密方式 Ea，將經加密處理後之含有硬體序號 S735、S745 的資料，經由傳輸網路 72 而傳送給檔案處理中心 71。檔案處理中心 71 之處理器 711 可執行檔案加/解密程式 714，配合記憶體 712 的運作，利用檔案處理中心 71 之私有鑰匙 Key716，對經非對稱性單向函數加密方式 Ea 所加密的電子檔案讀取裝置 73、74

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (15)

的硬體序號 S735、S745 訊息，進行解密而得出硬體序號 S735、S745，並將此些硬體序號 S735、S745 儲存於資料庫 717 內。

每一個電子檔案讀取裝置 73、74 均分別地包含處理器 731、741、記憶體 732、742、資料儲存媒體 733、743、以及螢幕 736、746，資料儲存媒體 733、743 分別含有讀取/傳接處理程式 734、744，資料儲存媒體 733、743 可為硬碟，磁片，光碟片，可抹除程式化唯讀記憶體 EPROM，電子式可抹除程式化唯讀記憶體 EEPROM，或快閃記憶體 Flash ROM，處理器 731、741 可為微處理器或中央處理器，處理器 731、741 可執行讀取/傳接處理程式 734、744，以進行上述之讀取/傳接處理模組之工作。經由傳輸網路 72，而得到檔案處理中心 71 的公開鑰匙 Key715；當電子檔案讀取裝置 73、74 對檔案處理中心 71，進行資料、檔案上傳時，處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，利用其本身之電子檔案讀取裝置的硬體序號 S735、S745、以及對稱性加密方式 Es，來對上傳檔案做加密，電子檔案讀取裝置 73、74 將此加密後之檔案，經由傳輸網路 72 而傳至檔案處理中心 71；於進行電子檔案下載時，處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，利用電子檔案讀取裝置 73、74 之硬體序號 S735、S745，以對稱性解密方式 Ds，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案分別展現於電子檔案讀取裝置

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (16)

73、74 之螢幕 736、746 上，而當解密讀取完成後，於儲存檔案時，處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，仍用電子檔案讀取裝置 73、74 之硬體序號 S735、S745，將已解密讀取之檔案予以加密並做儲存，可儲存於電子檔案讀取裝置 73、74 資料儲存媒體 733、743 中。

第 5 圖為一示意圖，用以更詳細地解釋於第 3 圖中之電子檔案傳輸系統，進行電子檔案傳輸方法時之資料流向。如圖中所示，電子檔案傳輸系統 2 之檔案處理中心 3 以及電子檔案讀取裝置 5、6，經由傳輸網路 4 做網路連結，檔案處理中心 3 將其公開鑰匙 Key32 傳送給電子檔案讀取裝置 5，此公開鑰匙 Key32 之資料流向，以資料流向 A1 表示；而檔案處理中心 3 將其公開鑰匙 Key32 傳送給電子檔案讀取裝置 6，此公開鑰匙 Key32 之資料流向，以資料流向 A2。

待電子檔案讀取裝置 5、6，接收到此公開鑰匙 Key32 後，分別以讀取/接收處理模組 51、61 以及此公開鑰匙 Key32，並分別以非對稱單向函數加密方式 Ea-5、以及 Ea-6，來對電子檔案讀取裝置 5 之硬體序號 S52、以及電子檔案讀取裝置 6 之硬體序號 S62 予以加密，並將加密後之資料 Ea-5(S52)、Sa-6(S62)傳送給檔案處理中心 3。資料流向 A3 表示，加密之 Ea-5(S52)資料之流向，由電子檔案讀取裝置 5 傳送給檔案處理中心 3；資料流向 A4 表示，加密之 Ea-6(S62)資料之流向，由電子檔案讀取裝

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (17)

置 6 傳送給檔案處理中心 3。

檔案處理中心 3 接收到來自電子檔案讀取裝置 5、6 之加密資料 Ea-5(S52)、以及 Ea-6(S62)後，將利用檔案加/解密模組 31、私有鑰匙 Key33、以及非對稱單向函數解密方式 Da-5、Da-6，對加密資料 Ea-5(S52)、以及 Ea-6(S62)，進行解密 Da-5(Ea-5(S52))、Da-6(Ea-6(S62))，得出 Da-5(Ea-5(S52))=S52、Da-6(Ea-6(S62))Da=S62，而得出硬體序號 S52、S62，並將此些硬體序號 S52、S62 儲存於資料庫 34 內。

於進行檔案上傳過程時，電子檔案讀取裝置 5、6 之讀取/接傳處理模組 51、61，將利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性加密方式 Es-5、Es-6，來對上傳檔案 m、n 做加密，而成為加密檔案 Es-5(m)、Es-6(n)，電子檔案讀取裝置 5、6，將此加密後之檔案 Es-5(m)、Es-6(n)，經由傳輸網路 4 而傳至檔案處理中心 3。資料流向 A5，表示加密後之檔案 Es-5(m)，自電子檔案讀取裝置 5 經由傳輸網路 4 而傳至檔案處理中心 3；資料流向 A6，表示加密後之檔案 Es-6(n)，自電子檔案讀取裝置 6 經由傳輸網路 4 而傳至檔案處理中心 3。

檔案處理中心 3 接收到此經硬體序號 S52、S62 加密之檔案 Es-5(m)、Es-6(n)後，將搜尋資料庫 34 以找出傳送端之電子檔案讀取裝置 5、6 所對應的硬體序號 S52、S62；利用檔案加/解密模組 31、電子檔案讀取裝置 5、6 所對應的硬體序號 S52、S62、以及對稱性解密方式 Ds-5、

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (18)

Ds-6，而對加密檔案 Es-5(m)、Es-6(n)予以解密，而 $Ds-5(Es-5(m))=m$ 、 $Ds-6(Es-6(n))=n$ ，得出檔案 m、n 內容。

於進行檔案下傳過程時，檔案處理中心 3 將依提出檔案下載請求之電子檔案讀取裝置 5、6 的硬體序號 S52、S62，利用檔案加/解密模組 3-1，以電子檔案讀取裝置 5、6 的硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，來對電子檔案 p、q 做加密，使成為加密檔案 Es-5(p)、Es-6(q)，將此些經對稱性加密方式 Es-5、Es-6 所加密的電子檔案 Es-5(p)、Es-6(q)，經由傳輸網路 4，而分別傳送給電子檔案讀取裝置 5、6。資料流向 A7，表示加密後之檔案 Es-5(p)，自檔案處理中心 3 經由傳輸網路 4 而傳至電子檔案讀取裝置 5；資料流向 A8，表示加密後之檔案 Es-6(q)，自檔案處理中心 3 經由傳輸網路 4 而傳至電子檔案讀取裝置 6。

電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61，利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性解密方式 Ds-5、Ds-6，來對經加密之電子檔案 Es-5(p)、Es-6(q) 做解密讀取的動作，而得出 $Ds-5(Es-5(p))=p$ ， $Ds-6(Es-6(q))=q$ ，當解密讀取完成後，並將解密之檔案 p、q 分別展現於電子檔案讀取裝置 5、6 之螢幕 53、63 上，而當解密讀取完成後，於儲存 p、q 檔案時，讀取/傳送處理模組 51、61 仍用電子檔案讀取裝置 5、6 之硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，將已解密讀取之檔案 p、q 予以加

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (19)

密並做儲存，將已解密讀取之檔案 p、q 予以加密成 Es-5(p)、Es-6(q)並做儲存，於電子檔案讀取裝置 5 之使用者可將加密檔案 Es-5(p)儲存於記憶裝置 54，磁片 55，亦或光碟片 56 中。於電子檔案讀取裝置 5 之使用者無法將檔案 p(解密檔案型式)儲存於記憶裝置 54，磁片 55，亦或光碟片 56 內。

即便，當於電子檔案讀取裝置 6 之使用者，經由傳輸網路 4，以檔案傳輸協定 FTP 方式，自電子檔案讀取裝置 5 而將電子書加密檔案 Es-5(p)載入電子檔案讀取裝置 6 內；或是直接將載有電子書加密檔案 Es-5(p)之磁片 55 或光碟片 56，置入電子檔案讀取裝置 6 中，而載入電子書加密檔案 Es-5(p)。由於電子檔案讀取裝置 6 之硬體序號為 S62，並非為 S52，所以電子檔案讀取裝置 6 之讀取/傳接處理模組 61，無法以硬體序號 S62、以及對稱性解密方式 Ds-6，無法對自電子檔案讀取裝置 5 而來之電子書加密檔案 Es-5(p)進行解密讀取。同理，電子檔案讀取裝置 5 之硬體序號為 S52，並非為 S62，所以電子檔案讀取裝置 5 之電子書處理模組 51，無法以硬體序號 S52、以及對稱性解密方式 Ds-5，無法對自電子檔案讀取裝置 6 而來之電子書加密檔案 Es-6(q)進行解密讀取。

所以，利用本發明之電子檔案傳輸系統 2，以進行電子檔案傳輸方法時，於電子檔案讀取裝置 5、6 的使用者能上傳加密檔案 Es-5(m)、Es-6(n)、以及下載加密檔案 Es-5(p)、Es-6(q)，並且由於檔案之加密 Es-5、Es-6/解密

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (20)

Ds-5、Ds-6 方式，使得下載之加密檔案 Es-5(p)、Es-6(q)，僅能分別於接收端之電子檔案讀取裝置 5、6 上，才能予以解密並讀取，而當解密讀取完成後，於儲存檔案時，仍分別用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，將已解密讀取之檔案予以加密，成為加密檔案 Es-5(p)、Es-6(q)並做儲存，而並非以解密檔案 p、q 的型式將檔案予以儲存，而能達到防止數位化資訊無限制的做複製拷貝、並做再次傳輸散播的目的。

對於第 4 圖中之電子檔案傳輸系統而言，其進行電子檔案傳輸方法時之資料流向與第 5 圖中之資料流向同理，所以在此不再贅述。

第 6 圖為一運作流程圖，其中顯示應用本發明之電子檔案傳輸系統以進行電子檔案傳輸方法的流程程序。如第 6 圖中所示，首先於步驟 21，進行註冊啟始程序，檔案處理中心 3 將得到電子檔案讀取裝置 5、6 之硬體序號 S52、S62，接著進到步驟 22。

於步驟 22，進行電子檔案傳輸程序，電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61，利用電子檔案讀取裝置 5、6 的硬體序號 S52、S62，並以對稱性加密方式 Ea-5、Ea-6、對稱性解密方式 Da-5、Da-6，來對檔案做加/解密動作，於檔案處理中心 3 與電子檔案讀取裝置 5、6 之間，進行電子檔案傳輸，並進到步驟 23。

於步驟 23，結束電子檔案傳輸過程。

第 7 圖為一運作流程圖，其中顯示於第 6 圖中之進行

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (21)

註冊啟始步驟之流程程序。如第 7 圖中所示，首先，於步驟 211，電子檔案傳輸系統 2 之檔案處理中心 3 以及電子檔案讀取裝置 5、6，經由傳輸網路 4 做網路連結，檔案處理中心 3 將其公開鑰匙 Key32 傳送給電子檔案讀取裝置 5、6，並進到步驟 212。

於步驟 212，待電子檔案讀取裝置 5、6，接收到此公開鑰匙 Key32 後，分別以讀取/接收處理模組 51、61 以及此公開鑰匙 Key32，並分別以非對稱單向函數加密方式 Ea-5、以及 Ea-6，來對電子檔案讀取裝置 5 之硬體序號 S52、以及電子檔案讀取裝置 6 之硬體序號 S62 予以加密，並將加密後之資料 Ea-5(S52)、Sa-6(S62)傳送給檔案處理中心 3，並進到步驟 213。

於步驟 213，檔案處理中心 3 接收到來自電子檔案讀取裝置 5、6 之加密資料 Ea-5(S52)、以及 Ea-6(S62)後，將利用檔案加/解密模組 31、私有鑰匙 Key33、以及非對稱單向函數解密方式 Da-5、Da-6，對加密資料 Ea-5(S52)、以及 Ea-6(S62)，進行解密 Da-5(Ea-5(S52))、Da-6(Ea-6(S62))，得出 Da-5(Ea-5(S52))=S52、Da-6(Ea-6(S62))Da=S62，而得出硬體序號 S52、S62，並將此些硬體序號 S52、S62 儲存於資料庫 34 內。

第 8 圖為一運作流程圖，其中顯示於第 6 圖中之進行電子檔案傳輸步驟之流程程序。如第 8 圖中所示，首先，於步驟 221，判斷為電子檔案讀取裝置 5、6 向檔案處理中心，提出下載電子檔案請求，以進行檔案下傳程序，亦

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (22)

或為電子檔案讀取裝置 5、6 上傳檔案至檔案處理中心，以進行檔案上傳程序；若為進行檔案下傳程序，則進到步驟 222，若為檔案上傳程序，則進到步驟 226。

於步驟 222，進行檔案下傳，檔案處理中心 3 將依提出檔案下載請求之電子檔案讀取裝置 5、6 的硬體序號 S52、S62，利用檔案加/解密模組 31，以儲存於資料庫 34 之電子檔案讀取裝置 5、6 硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，來對電子檔案 p、q 做加密，使成為加密檔案 Es-5(p)、Es-6(q)，將此些經對稱性加密方式 Es-5、Es-6 所加密的電子檔案 Es-5(p)、Es-6(q)，經由傳輸網路 4，而分別傳送給電子檔案讀取裝置 5、6，並進到步驟 223。

於步驟 223，電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61，利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性解密方式 Ds-5、Ds-6，來對經加密之電子檔案 Es-5(p)、Es-6(q) 做解密讀取的動作，而得出 $Ds-5(Es-5(p))=p$ ， $Ds-6(Es-6(q))=q$ ，並將解密之檔案 p、q 分別展現於電子檔案讀取裝置 5、6 之螢幕 53、63 上，進到步驟 224。

於步驟 224，當解密讀取完成後，於儲存 p、q 檔案時，讀取/傳送處理模組 51、61 仍用電子檔案讀取裝置 5、6 之硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，將已解密讀取之檔案 p、q 予以加密並做儲存，將已解密讀取之檔案 p、q 予以

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (23)

加密成 Es-5(p)、Es-6(q)並做儲存，於電子檔案讀取裝置 5、6 之使用者可將加密檔案 Es-5(p)、Es-6(q)分別儲存於記憶裝置 54、6，磁片 55、65，亦或光碟片 56、66 中，並進到步驟 225。

於步驟 225，電子檔案讀取裝置 5、6 是否繼續進行上傳檔案，或下載電子檔案動作，若繼續進行，則回到步驟 221；若結束電子檔案傳輸，則進到步驟 228。

於步驟 226，進行檔案上傳，電子檔案讀取裝置 5、6 之讀取/接傳處理模組 51、61，將利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性加密方式 Es-5、Es-6，來對上傳檔案 m、n 做加密，而成為加密檔案 Es-5(m)、Es-6(n)，電子檔案讀取裝置 5、6，將此加密後之檔案 Es-5(m)、Es-6(n)，經由傳輸網路 4 而傳至檔案處理中心 3，並進到步驟 227。

於步驟 227，檔案處理中心 3 接收到此經硬體序號 S52、S62 加密之檔案 Es-5(m)、Es-6(n)後，將搜尋資料庫 34 以找出傳送端之電子檔案讀取裝置 5、6 所對應的硬體序號 S52、S62；利用檔案加/解密模組 31、電子檔案讀取裝置 5、6 所對應的硬體序號 S52、S62、以及對稱性解密方式 Ds-5、Ds-6，而對加密檔案 Es-5(m)、Es-6(n)予以解密，而 $Ds-5(Es-5(m))=m$ 、 $Ds-6(Es-6(n))=n$ ，得出檔案 m、n 內容，並進到步驟 225。

於步驟 228，電子檔案讀取裝置 5、6 與檔案處理中心間，停止上傳檔案、以及下載電子檔案。

(請先閱讀請背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (24)

於第 6 圖、第 7 圖、以及第 8 圖之電子檔案傳輸方法的運作流程程序，雖然乃應用於，如第 3 圖中之本發明之電子檔案傳輸系統之一實施例，但是此電子檔案傳輸方法的運作流程程序，同理，可適用於如第 4 圖中之本發明之電子檔案傳輸系統之另一實施例，在此，不再贅述。

第 9 圖為一運作流程圖，其中顯示應用如第 3 圖中之電子檔案傳輸系統之實施例，以進行電子檔案傳輸方法的一流程程序。如圖中所示，首先，於步驟 311，電子檔案傳輸系統 2 之檔案處理中心 3 以及電子檔案讀取裝置 5、6，經由傳輸網路 4 做網路連結，檔案處理中心 3 將其公開鑰匙 Key32 傳送給電子檔案讀取裝置 5、6，並進到步驟 312。

於步驟 312，待電子檔案讀取裝置 5、6，接收到此公開鑰匙 Key32 後，分別以讀取/接收處理模組 51、61 以及此公開鑰匙 Key32，並分別以非對稱單向函數加密方式 Ea-5、以及 Ea-6，來對電子檔案讀取裝置 5 之硬體序號 S52、以及電子檔案讀取裝置 6 之硬體序號 S62 予以加密，並將加密後之資料 Ea-5(S52)、Sa-6(S62)傳送給檔案處理中心 3，並進到步驟 313。

於步驟 313，檔案處理中心 3 接收到來自電子檔案讀取裝置 5、6 之加密資料 Ea-5(S52)、以及 Ea-6(S62)後，將利用檔案加/解密模組 31、私有鑰匙 Key33、以及非對稱單向函數解密方式 Da-5、Da-6，對加密資料 Ea-5(S52)、以及 Ea-6(S62)，進行解密 Da-5(Ea-5(S52))、Da-6(Ea-

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (25)

6(S62))，得出 $Da-5(Ea-5(S52))=S52$ 、 $Da-6(Ea-6(S62))Da=S62$ ，而得出硬體序號 S52、S62，並將此些硬體序號 S52、S62 儲存於資料庫 34 內，並進到步驟 314。

於步驟 314，進行檔案下傳，檔案處理中心 3 將依提出檔案下載請求之電子檔案讀取裝置 5、6 的硬體序號 S52、S62，利用檔案加/解密模組 31，以儲存於資料庫 34 之電子檔案讀取裝置 5、6 硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，來對電子檔案 p、q 做加密，使成為加密檔案 Es-5(p)、Es-6(q)，將此些經對稱性加密方式 Es-5、Es-6 所加密的電子檔案 Es-5(p)、Es-6(q)，經由傳輸網路 4，而分別傳送給電子檔案讀取裝置 5、6，並進到步驟 315。

於步驟 315，電子檔案讀取裝置 5、6 之讀取/傳接處理模組 51、61，利用電子檔案讀取裝置 5、6 之硬體序號 S52、S62，以對稱性解密方式 Ds-5、Ds-6，來對經加密之電子檔案 Es-5(p)、Es-6(q) 做解密讀取的動作，而得出 $Ds-5(Es-5(p))=p$ ， $Ds-6(Es-6(q))=q$ ，並將解密之檔案 p、q 分別展現於電子檔案讀取裝置 5、6 之螢幕 53、63 上，進到步驟 316。

於步驟 316，當解密讀取完成後，於儲存 p、q 檔案時，讀取/傳送處理模組 51、61 仍用電子檔案讀取裝置 5、6 之硬體序號 S52、S62 當成加密鑰匙 KeyS52、KeyS62，並利用對稱性加密方式 Es-5、Es-6，將已解密讀取之檔案 p、q 予以加密並做儲存，將已解密讀取之檔案 p、q 予以

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (26)

加密成 $Es-5(p)$ 、 $Es-6(q)$ 並做儲存，於電子檔案讀取裝置 5、6 之使用者可將加密檔案 $Es-5(p)$ 、 $Es-6(q)$ 分別儲存於記憶裝置 54、6，磁片 55、65，亦或光碟片 56、66 中，並進到步驟 317。

於步驟 317，進行檔案上傳，電子檔案讀取裝置 5、6 之讀取/接傳處理模組 51、61，將利用電子檔案讀取裝置 5、6 之硬體序號 $S52$ 、 $S62$ ，以對稱性加密方式 $Es-5$ 、 $Es-6$ ，來對上傳檔案 m 、 n 做加密，而成為加密檔案 $Es-5(m)$ 、 $Es-6(n)$ ，電子檔案讀取裝置 5、6，將此加密後之檔案 $Es-5(m)$ 、 $Es-6(n)$ ，經由傳輸網路 4 而傳至檔案處理中心 3，並進到步驟 318。

於步驟 318，檔案處理中心 3 接收到此經硬體序號 $S52$ 、 $S62$ 加密之檔案 $Es-5(m)$ 、 $Es-6(n)$ 後，將搜尋資料庫 34 以找出傳送端之電子檔案讀取裝置 5、6 所對應的硬體序號 $S52$ 、 $S62$ ；利用檔案加/解密模組 31、電子檔案讀取裝置 5、6 所對應的硬體序號 $S52$ 、 $S62$ 、以及對稱性解密方式 $Ds-5$ 、 $Ds-6$ ，而對加密檔案 $Es-5(m)$ 、 $Es-6(n)$ 予以解密，而 $Ds-5(Es-5(m))=m$ 、 $Ds-6(Es-6(n))=n$ ，得出檔案 m 、 n 內容，並進到步驟 319。

於步驟 319，電子檔案讀取裝置 5、6 與檔案處理中心 3 間，停止上傳檔案、以及下載電子檔案。

第 10 圖為一運作流程圖，其中顯示應用如第 4 圖中之電子檔案傳輸系統之實施例，以進行電子檔案傳輸方法的另一流程程序。如圖中所示，於步驟 411，電子檔案傳

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (27)

輸系統 7 之檔案處理中心 71 以及電子檔案讀取裝置 73、74，經由傳輸網路 72 做網路連結，檔案處理中心 71 將其公開鑰匙 Key715 傳送給電子檔案讀取裝置 73、74，並進到步驟 412。

於步驟 412，待電子檔案讀取裝置 73、74，接收到此公開鑰匙 Key715 後，電子檔案讀取裝置 73、74 之處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，利用檔案處理中心 3 所發行之公開鑰匙 Key715、以非對稱性單向函數加密方式 Ea-5、Ea-6，來對電子檔案讀取裝置 73、74 之硬體序號 S735、S745 予以加密，並將加密後之資料 Ea-5(S735)、Sa-6(S745)，經由傳輸網路 72，傳送給檔案處理中心 71，並進到步驟 413。

於步驟 413，檔案處理中心 71 接收到來自電子檔案讀取裝置 73、74 之加密資料 Ea-5(S735)、以及 Ea-6(S745) 後，檔案處理中心 71 之處理器 711 可執行檔案加/解密程式 714，配合記憶體 712 的運作，利用檔案處理中心 71 之私有鑰匙 Key716、以及非對稱單向函數解密方式 Da-5、Da-6，對加密資料 Ea-5(S735)、以及 Ea-6(S745)，進行解密 Da-5(Ea-5(S735))、Da-6(Ea-6(S745))，得出 Da-5(Ea-5(S735))=S735、Da-6(Ea-6(S745))Da=S745，而得出硬體序號 S735、S745，並將此些硬體序號儲存於資料庫 717 內，並進到步驟 414。

於步驟 414，進行檔案上傳，處理器 731、741 可執

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (28)

行讀取/傳接處理程式 734、744，配合記憶體 732、742，利用其本身之電子檔案讀取裝置 73、74 的硬體序號 S735、S745、以及對稱性加密方式 Es-5、Es-6，來對上傳檔案 m、n 做加密，而成為加密檔案 Es-5(m)、Es-6(n)，電子檔案讀取裝置 73、74，將此加密後之檔案 Es-5(m)、Es-6(n)，經由傳輸網路 72 而傳至檔案處理中心 71，並進到步驟 415。

於步驟 415，檔案處理中心 71 接收到來自電子檔案讀取裝置 73、74 之加密檔案 Es-5(m)、Es-6(n)後，檔案處理中心 71 之處理器 711 可執行檔案加/解密程式 714，配合記憶體 712 的運作，利用檔案處理中心 71 之私有鑰匙 Key716、以及非對稱單向函數解密方式 Da-5、Da-6，而對加密檔案 Es-5(m)、Es-6(n)予以解密，而 $Ds-5(Es-5(m))=m$ 、 $Ds-6(Es-6(n))=n$ ，得出檔案 m、n 內容，並進到步驟 416。

於步驟 416，進行檔案下傳，檔案處理中心 71 之處理器 711 可執行檔案加/解密程式 714，配合記憶體 712 的運作，以儲存於資料庫 717 之電子檔案讀取裝置 73、74 之硬體序號 S735、S745 當成加密鑰匙 KeyS735、KeyS745，並利用對稱性加密方式 Es-5、Es-6，來對電子檔案 p、q 做加密，使成為加密檔案 Es-5(p)、Es-6(q)，將此些經對稱性加密方式 Es-5、Es-6 所加密的電子檔案 Es-5(p)、Es-6(q)，經由傳輸網路 72，而分別傳送給電子檔案讀取裝置 73、74，並進到步驟 417。

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (29)

於步驟 417，電子檔案讀取裝置 73、74 之處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，利用電子檔案讀取裝置 73、74 之硬體序號 S735、S745，以對稱性解密方式 $Ds-5$ 、 $Ds-6$ ，來對經加密之電子檔案 $Es-5(p)$ 、 $Es-6(q)$ 做解密讀取的動作，而得出 $Ds-5(Es-5(p))=p$ ， $Ds-6(Es-6(q))=q$ ，並將解密之檔案 p 、 q 分別展現於電子檔案讀取裝置 73、74 之螢幕 736、746 上，進到步驟 418。

於步驟 418，當解密讀取完成後，於儲存 p 、 q 檔案時，處理器 731、741 可執行讀取/傳接處理程式 734、744，配合記憶體 732、742，仍用電子檔案讀取裝置 73、74 之硬體序號 S735、S745 當成加密鑰匙 $KeyS735$ 、 $KeyS745$ ，並利用對稱性加密方式 $Es-5$ 、 $Es-6$ ，將已解密讀取之檔案 p 、 q 予以加密並做儲存，將已解密讀取之檔案 p 、 q 予以加密成 $Es-5(p)$ 、 $Es-6(q)$ 並做儲存，可儲存於電子檔案讀取裝置 73、74 資料儲存媒體 733、743 中，並進到步驟 419。

於步驟 419，電子檔案讀取裝置 73、74 與檔案處理中心 71 間，停止上傳檔案、以及下載電子檔案。

綜合以上的實施例，可知本發明之電子檔案傳輸系統及方法的優點為：由於檔案之加密/解密方式，使得下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，於儲存檔案時，仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，而並非以解密檔案的型式將檔案予以

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

五、發明說明 (30)

儲存。同時，能達到防止數位化資訊無限制的做複製拷貝、並做再次傳輸散播的目的。

以上所述僅為本發明之較佳實施例而已，並非用以限定本發明之範圍；凡其它未脫離本發明所揭示之精神下所完成之等效改變或修飾，均應包含在下述之專利範圍內。

元件符號之說明

11,15	訊息伺服器
111,151	網站
112,152	電子書讀取軟體
113,153	電子檔案
12,16	網際網路
13,14,17,18	個人電腦
131,171	磁片
132,172	光碟片
154	加密檔案

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

1. 一種電子檔案傳輸方法，係應用於包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置的電子檔案傳輸系統，以當電子檔案經由網路進行傳輸時，使該電子檔案讀取裝置具有一硬體序號並予以加密，俾令電子檔案讀取裝置下載之加密檔案，僅能於接收端之電子檔案讀取裝置上，才能予以解密並讀取，而當解密讀取完成後，儲存檔案時，仍用電子檔案讀取裝置之硬體序號，將已解密讀取之檔案予以加密並做儲存，此電子檔案傳輸方法包含以下程序：

(1)進行電子檔案傳輸程序，令檔案處理中心利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對檔案做加/解密動作，以於檔案處理中心與電子檔案讀取裝置之間進行電子檔案傳輸；以及

(2)結束電子檔案傳輸。

2. 如申請專利範圍第 1 項所述之電子檔案傳輸方法，其中，該程序(1)之進行電子檔案傳輸程序包含以下步驟：

判斷為電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求以進行檔案下傳程序，亦或為電子檔案讀取裝置上傳檔案至檔案處理中心以進行檔案上傳程序；若為進行檔案下傳程序，則利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對下載檔案做加/解密動作，以於檔案處理中

(請先閱讀背面之注意事項再填寫本頁)

訂

線

六、申請專利範圍

心與電子檔案讀取裝置之間，進行電子檔案下載傳輸；若為進行檔案上傳程序，則利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對上傳檔案做加/解密動作，以於檔案處理中心與電子檔案讀取裝置之間，進行電子檔案上傳傳輸。

3. 如申請專利範圍第2項所述之電子檔案傳輸方法，其中，該進行檔案下載程序包含以下步驟：

令電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求進行檔案下傳，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，利用檔案加/解密模組，以儲存於資料庫之電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式來對電子檔案做加密，將此加密的電子檔案，經由傳輸網路而傳送給電子檔案讀取裝置；

使電子檔案讀取裝置之讀取/傳接處理模組利用電子檔案讀取裝置之硬體序號，以對稱性解密方式來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上；

當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式，將已解密讀取之檔案予以加密並做儲存；以及

電子檔案讀取裝置決定是否繼續進行下載電子檔案動作。

六、申請專利範圍

4. 如申請專利範圍第2項所述之電子檔案傳輸方法，其中，該進行檔案上傳程序包含以下步驟：

令電子檔案讀取裝置之讀取/接傳處理模組利用電子檔案讀取裝置之硬體序號，以對稱性加密方式，來對上傳檔案做加密，將此加密後之檔案經由傳輸網路而傳至檔案處理中心；

檔案處理中心接收到此經硬體序號加密之檔案後，將搜尋資料庫以找出傳送端之電子檔案讀取裝置所對應的硬體序號；利用檔案加/解密模組、電子檔案讀取裝置所對應的硬體序號、以及對稱性解密方式，而得出檔案內容；以及

電子檔案讀取裝置決定是否繼續進行上傳電子檔案動作。

5. 一種電子檔案傳輸方法，係應用於包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置的電子書傳輸系統，該電子檔案讀取裝置並具有一硬體序號，此電子檔案傳輸方法包含以下程序：

(1)電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求進行檔案下傳，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，利用檔案加/解密模組，以儲存於資料庫之電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式，來對電子檔案做加密，然後將此加密的電子檔案經由傳輸網路而傳送給電子檔案讀取裝置；

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

(2)令電子檔案讀取裝置之讀取/傳接處理模組，利用電子檔案讀取裝置之硬體序號，以對稱性解密方式，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上；

(3)當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式，將已解密讀取之檔案予以加密並做儲存；以及

(4)電子檔案讀取裝置結束下載電子檔案動作。

6. 如申請專利範圍第5項所述之電子檔案傳輸方法，其中該程序(1)進行前復包括下列步驟：

令電子檔案傳輸系統之檔案處理中心以及電子檔案讀取裝置經由傳輸網路做網路連結，以由檔案處理中心將其公開鑰匙傳送給電子檔案讀取裝置；

待電子檔案讀取裝置接收到此公開鑰匙後，以讀取/接收處理模組以及此公開鑰匙，並以非對稱單向函數加密方式，來對電子檔案讀取裝置之硬體序號予以加密，並將加密後之資料傳送給檔案處理中心；以及

檔案處理中心接收到來自電子檔案讀取裝置之加密資料後，將利用檔案加/解密模組、私有鑰匙、以及非對稱單向函數解密方式，對加密資料進行解密，而得出電子讀取裝置之硬體序號，並將此些硬體序號儲存於資料庫內。

7. 一種電子檔案傳輸方法，係應用於包含檔案處理中心、

六、申請專利範圍

傳輸網路、以及電子檔案讀取裝置的電子書傳輸系統，該電子檔案讀取裝置並具有一硬體序號，此電子檔案傳輸方法包含以下程序；

(1)令電子檔案讀取裝置之讀取/接傳處理模組利用電子檔案讀取裝置之硬體序號，以對稱性加密方式，來對上傳檔案做加密，將此加密後之檔案，經由傳輸網路而傳至檔案處理中心；

(2)檔案處理中心接收到此經硬體序號加密之檔案後，將搜尋資料庫以找出傳送端之電子檔案讀取裝置所對應的硬體序號；利用檔案加/解密模組、電子檔案讀取裝置所對應的硬體序號、以及對稱性解密方式，而得出檔案內容；以及

(3)電子檔案讀取裝置結束上傳電子檔案動作。

8. 如申請專利範圍第 7 項所述之電子檔案讀取裝置，其中，於該程序(1)進行前復包括下列步驟：

令電子檔案傳輸系統之檔案處理中心以及電子檔案讀取裝置經由傳輸網路做網路連結，以由檔案處理中心將其公開鑰匙傳送給電子檔案讀取裝置；

待電子檔案讀取裝置接收到此公開鑰匙後，以讀取/接收處理模組以及此公開鑰匙，並以非對稱單向函數加密方式，來對電子檔案讀取裝置之硬體序號予以加密，並將加密後之資料傳送給檔案處理中心；以及

檔案處理中心接收到來自電子檔案讀取裝置之加密資料後，將利用檔案加/解密模組、私有鑰匙、以及

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

非對稱單向函數解密方式，對加密資料進行解密，而得出電子讀取裝置之硬體序號，並將此些硬體序號儲存於資料庫內。

9. 一種電子檔案傳輸方法，係應用於包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置的電子書傳輸系統，該電子檔案讀取裝置並具有一硬體序號，此電子檔案傳輸方法包含以下程序：

(1)進行註冊啟始程序，以令檔案處理中心取得該電子檔案讀取裝置之硬體序號；

(2)進行電子檔案傳輸程序，以利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對檔案做加/解密動作，而於檔案處理中心與電子檔案讀取裝置之間進行電子檔案傳輸；以及

(3)結束電子檔案傳輸過程。

10. 如申請專利範圍第9項所述之電子檔案傳輸方法，其中，該程序(1)之進行註冊啟始程序包含以下步驟：

令電子檔案傳輸系統之檔案處理中心以及電子檔案讀取裝置經由傳輸網路做網路連結，以使檔案處理中心將其公開鑰匙傳送給電子檔案讀取裝置；

待電子檔案讀取裝置接收到此公開鑰匙後，以讀取/接收處理模組以及此公開鑰匙，並以非對稱單向函數加密方式，對電子檔案讀取裝置之硬體序號予以加密，並將加密後之資料傳送給檔案處理中心；以及

檔案處理中心接收到來自電子檔案讀取裝置之加

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

密資料後，利用檔案加/解密模組、私有鑰匙、以及非對稱單向函數解密方式，對加密資料進行解密，而得出電子讀取裝置之硬體序號，並將此些硬體序號儲存於資料庫內。

11. 如申請專利範圍第 9 項所述之電子檔案傳輸方法，其中，該程序(2)之進行電子檔案傳輸程序包含以下步驟：

判斷為電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求以進行檔案下傳程序，亦或為電子檔案讀取裝置上傳檔案至檔案處理中心以進行檔案上傳程序；若為進行檔案下傳程序，則利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對下載檔案做加/解密動作，俾於檔案處理中心與電子檔案讀取裝置之間進行電子檔案下載傳輸；若為進行檔案上傳程序，則利用電子檔案讀取裝置的硬體序號，並以對稱性加密方式及對稱性解密方式，來對上傳檔案做加/解密動作，俾於檔案處理中心與電子檔案讀取裝置之間，進行電子檔案上傳傳輸。

12. 如申請專利範圍第 11 項所述之電子檔案傳輸方法，其中，該進行檔案下載程序包含以下步驟：

電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求進行檔案下傳時，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，利用檔案加/解密模組，以儲存於資料庫之電子檔案讀取裝置

(請先閱讀背面之注意事項再填寫本頁)

訂

線

六、申請專利範圍

之硬體序號當成加密鑰匙，並利用對稱性加密方式，來對電子檔案做加密，然後將此加密的電子檔案，經由傳輸網路而傳送給電子檔案讀取裝置；

令電子檔案讀取裝置之讀取/傳接處理模組利用電子檔案讀取裝置之硬體序號，以對稱性解密方式，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上；

當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式，將已解密讀取之檔案予以加密並做儲存；以及

電子檔案讀取裝置決定是否繼續進行下載電子檔案動作。

13. 如申請專利範圍第 11 項所述之電子檔案傳輸方法，其中，該進行檔案上傳程序包含以下步驟：

令電子檔案讀取裝置之讀取/接傳處理模組利用電子檔案讀取裝置之硬體序號，以對稱性加密方式，來對上傳檔案做加密，然後將此加密後之檔案經由傳輸網路而傳至檔案處理中心；

檔案處理中心接收到此經硬體序號加密之檔案後，將搜尋資料庫以找出傳送端之電子檔案讀取裝置所對應的硬體序號；利用檔案加/解密模組、電子檔案讀取裝置所對應的硬體序號、以及對稱性解密方式，而得出檔案內容；以及

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

電子檔案讀取裝置決定是否繼續進行上傳電子檔案動作。

14. 一種電子檔案傳輸方法，係應用於包含檔案處理中心、傳輸網路、以及電子檔案讀取裝置的電子書傳輸系統，該電子檔案讀取裝置並具有一硬體序號，此電子檔案傳輸方法包含以下程序：

(1)判斷為電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求以進行檔案下傳程序，亦或為電子檔案讀取裝置上傳檔案至檔案處理中心以進行檔案上傳程序；若為進行檔案下傳程序，則進到步驟(2)；若為檔案上傳程序，則進到步驟(6)；

(2)電子檔案讀取裝置向檔案處理中心提出下載電子檔案請求進行檔案下傳時，檔案處理中心將依提出檔案下載請求之電子檔案讀取裝置的硬體序號，利用檔案加/解密模組，以儲存於資料庫之電子檔案讀取裝置之硬體序號當成加密鑰匙，並利用對稱性加密方式，來對電子檔案做加密，將此加密的電子檔案，經由傳輸網路而傳送給電子檔案讀取裝置；

(3)電子檔案讀取裝置之讀取/傳接處理模組，利用電子檔案讀取裝置之硬體序號，以對稱性解密方式，來對經加密之電子檔案做解密讀取的動作，並將解密之檔案展現於電子檔案讀取裝置之螢幕上；

(4)當解密讀取完成後，於儲存檔案時，讀取/傳送處理模組仍用電子檔案讀取裝置之硬體序號當成加

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

六、申請專利範圍

密鑰匙，並利用對稱性加密方式，將已解密讀取之檔案予以加密並做儲存；

(5)判斷電子檔案讀取裝置是否繼續進行上傳檔案或下載電子檔案動作，若繼續進行，則回到步驟(1)；若結束電子檔案傳輸，則進到步驟(8)；

(6)進行檔案上傳時，令電子檔案讀取裝置之讀取/接傳處理模組利用電子檔案讀取裝置之硬體序號，以對稱性加密方式，來對上傳檔案做加密，並將此加密後之檔案經由傳輸網路而傳至檔案處理中心；

(7)檔案處理中心接收到此經硬體序號加密之檔案後，將搜尋資料庫以找出傳送端之電子檔案讀取裝置所對應的硬體序號；利用檔案加/解密模組、電子檔案讀取裝置所對應的硬體序號、以及對稱性解密方式，而得出檔案內容，並進到步驟(8)；以及

(8)令電子檔案讀取裝置與檔案處理中心間停止上傳檔案以及下載電子檔案。

15.如申請專利範圍第14項所述之電子檔案傳輸方法，其中於進行該程序(1)前復包括下列步驟：

令電子檔案傳輸系統之檔案處理中心以及電子檔案讀取裝置經由傳輸網路做網路連結，以由檔案處理中心將其公開鑰匙傳送給電子檔案讀取裝置；

待電子檔案讀取裝置接收到此公開鑰匙後，以讀取/接收處理模組以及此公開鑰匙，並以非對稱單向函數加密方式，來對電子檔案讀取裝置之硬體序號予以

(請先閱讀背面之注意事項再填寫本頁)

裝
訂
線

六、申請專利範圍

加密，並將加密後之資料傳送給檔案處理中心；以及
檔案處理中心接收到來自電子檔案讀取裝置之加密資料後，將利用檔案加/解密模組、私有鑰匙、以及非對稱單向函數解密方式，對加密資料進行解密，而得出電子讀取裝置之硬體序號，並將此些硬體序號儲存於資料庫內。

16. 一種電子檔案傳輸系統，係包括：

一個或一個以上之電子檔案讀取裝置，該電子檔案讀取裝置，具有一硬體序號，俾藉該硬體序號以對稱性加密方式，對上傳而出之電子檔案予以加密；並對於下載而來之加密電子檔案，利用其本身之硬體序號，以對稱性解密方式對下載之加密電子檔案予以解密讀取，且當解密讀取完成後，該電子檔案於儲存時，該電子檔案讀取裝置仍用其本身之硬體序號，將已解密讀取之電子檔案予以加密並做儲存，而非以解密檔案的型式將檔案予以儲存；

檔案處理中心，為進行數位化資訊服務的伺服平台，得提供其公開鑰匙給電子檔案讀取裝置，並可提供電子檔案，以供電子檔案讀取裝置進行檔案下載以及儲存自電子檔案讀取裝置而來之上傳檔案；檔案處理中心係包括：

資料庫，此資料庫用以儲存電子檔案讀取裝置之硬體序號；以及

檔案加/解密模組，此檔案加/解密模組利用檔案

(請先閱讀背面之注意事項再填寫本頁)

裝

訂

線

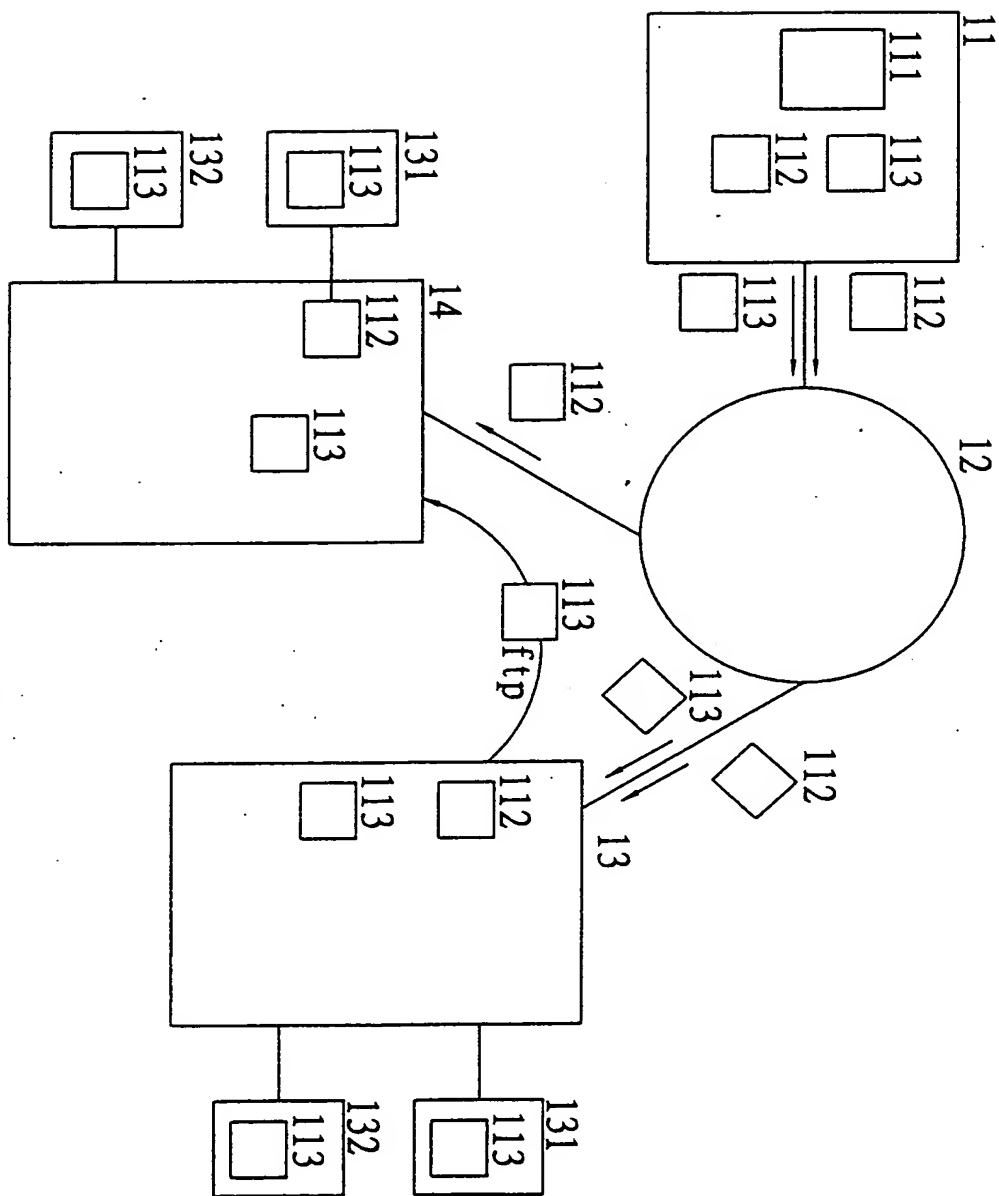
六、申請專利範圍

處理中心之私有鑰匙，以非對稱性解密方式，對來自電子檔案讀取裝置且含有電子檔案讀取裝置硬體序號的加密檔案予以解密，而將硬體序號儲存於資料庫；且得利用於資料庫中所儲存的硬體序號，以對稱性解密方式，對來自電子檔案讀取裝置之上傳加密檔案予以解密，而得出檔案內容；並且，該檔案加/解密模組可利用於資料庫中所儲存的硬體序號，以對稱性加密方式，將電子檔案讀取裝置所欲下載之電子檔案，予以加密後，再傳送給電子檔案讀取裝置；以及

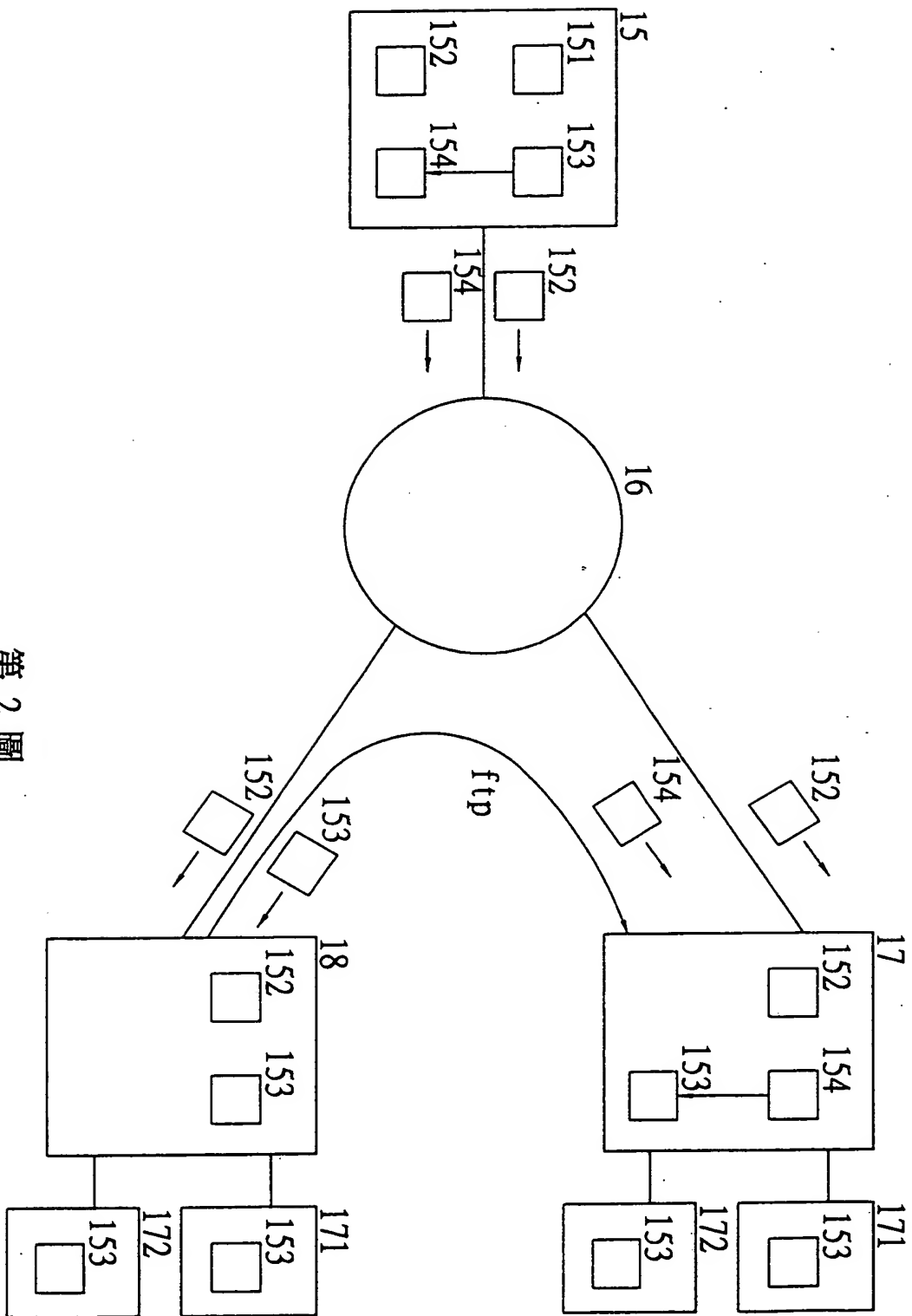
傳輸網路，將檔案處理中心與電子檔案讀取裝置予以網路連結。

(請先閱讀背面之注意事項再填寫本頁)

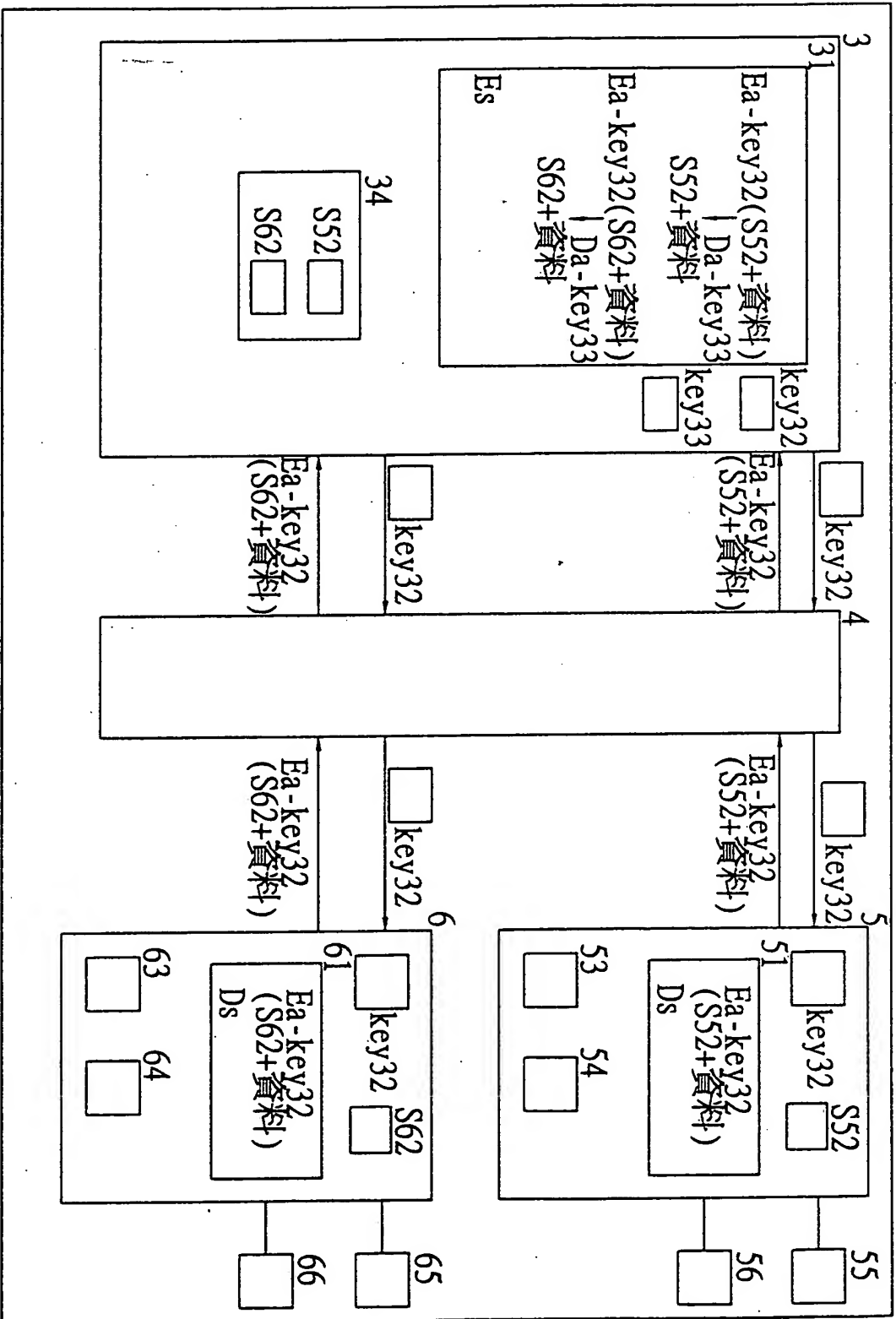
裝
訂
線



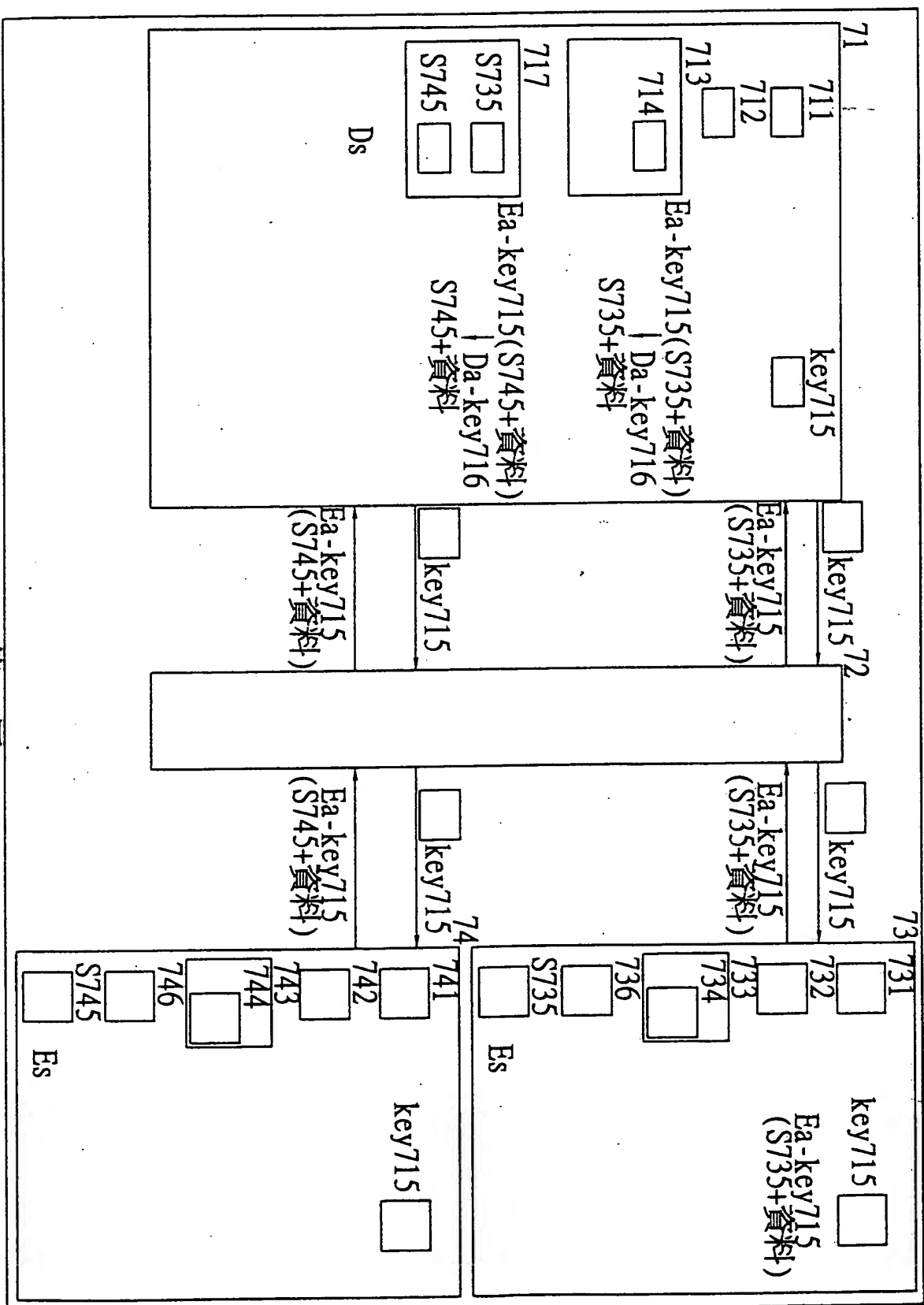
第 1 圖



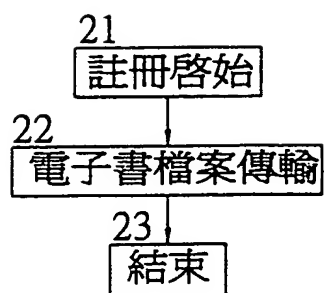
第 2 圖



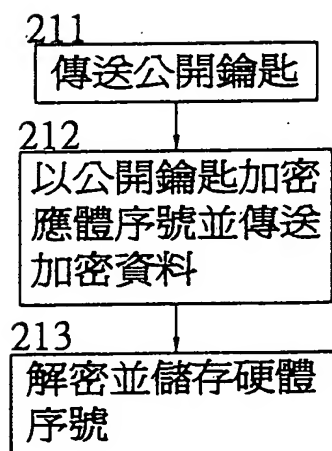
第 3 圖



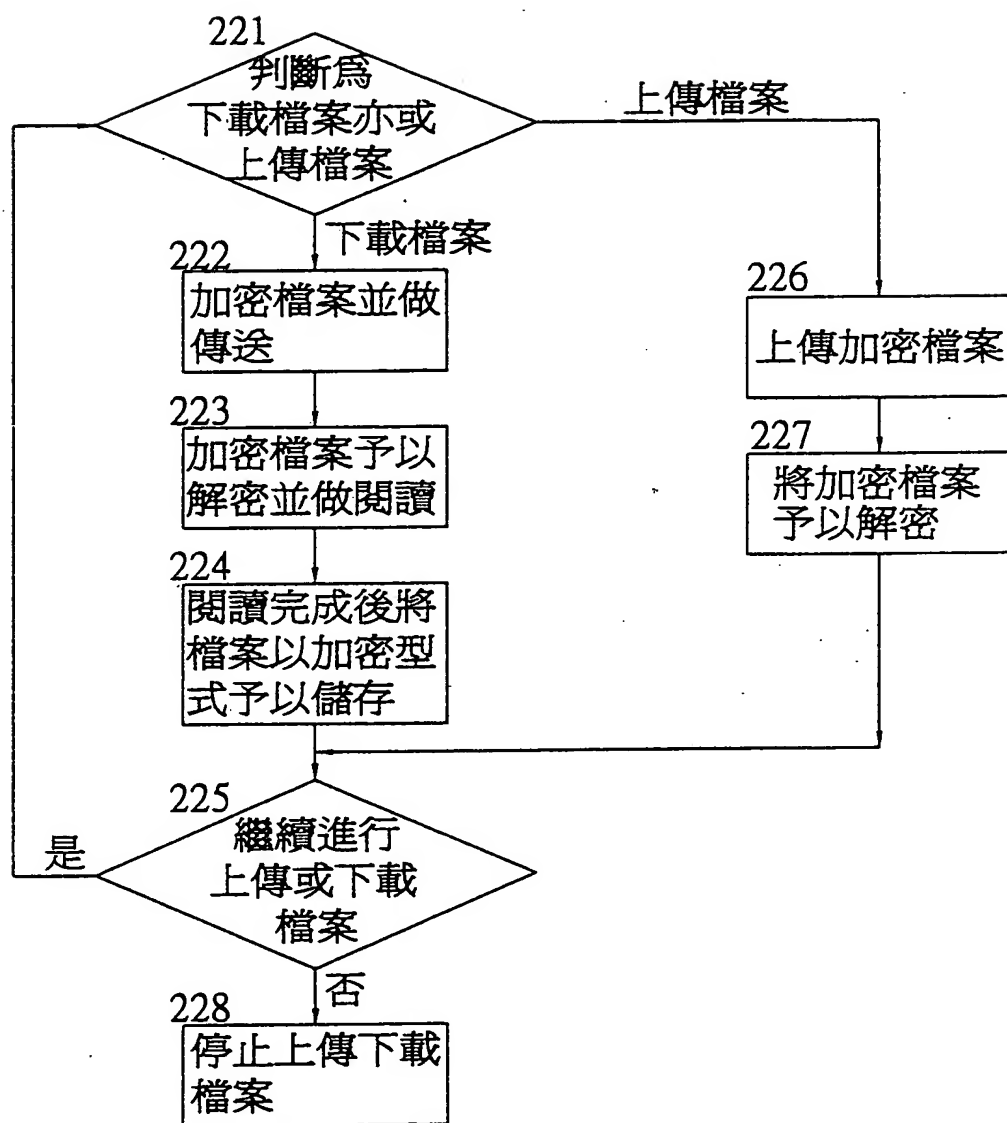
第 4 圖



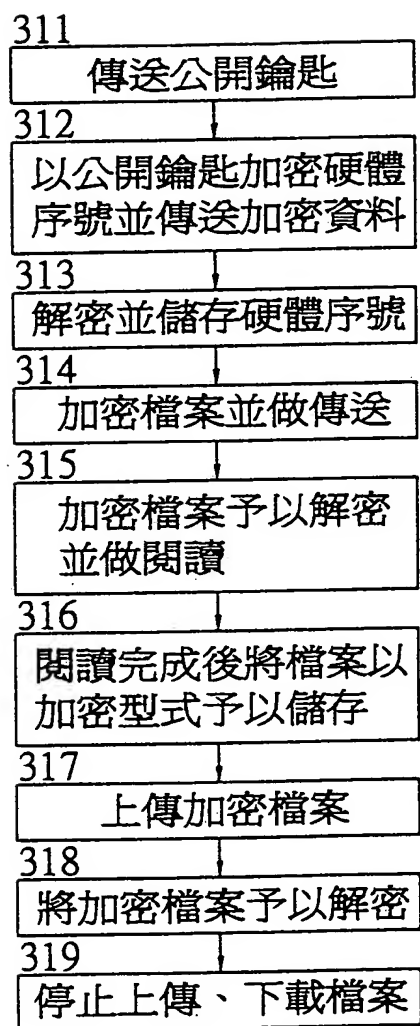
第 6 圖



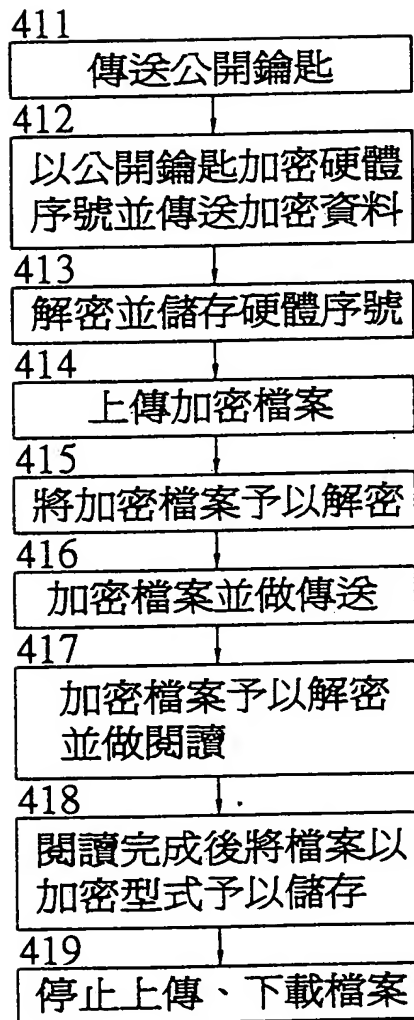
第 7 圖



第 8 圖



第 9 圖



第 10 圖